

ON THE STRUCTURE OF SUBSETS OF AN ORDERABLE GROUP WITH SOME SMALL DOUBLING PROPERTIES

G. A. FREIMAN, M. HERZOG, P. LONGOBARDI, M. MAJ,
A. PLAGNE, D. J. S. ROBINSON AND Y.V. STANCHESCU

1. INTRODUCTION

Let G denote an arbitrary group (multiplicatively written). If S is a subset of G , we define its *square* S^2 by the formula

$$S^2 = \{x_1x_2 \mid x_1, x_2 \in S\}.$$

In the abelian context, G will usually be additively written and we shall rather speak of *sumsets* and specifically of the *double* of S , namely

$$2S = \{x_1 + x_2 \mid x_1, x_2 \in S\}.$$

Here, we are concerned with the following general problem: for two real numbers $\alpha \geq 1$ and β , determine the *structure* of S if S is a finite subset of a group G satisfying an inequality on cardinalities of the form

$$|S^2| \leq \alpha|S| + \beta$$

when α is small and $|S|$ is typically large.

Problems of this kind are called *inverse problems* of *small doubling* type in additive number theory. The coefficient α (or more precisely the ratio $|S^2|/|S|$) is called the *doubling coefficient* of S . This type of problems became the most central issue in additive combinatorics. Inverse problems of small doubling type have been first investigated by G.A. Freiman very precisely in the additive group of the integers (see [4], [5], [6], [7]) and by many other authors in general abelian groups, starting with M. Kneser [16] (see, for example, [15], [17], [1], [23], [14]). More recently, small doubling problems in non-necessarily abelian groups have been also studied, see [13], [24] and [3] for recent surveys on these problems and [19] and [26] for two important books on the subject.

Keywords: Inverse problems; small doubling; nilpotent groups; ordered groups.

Mathematics Subject Classification 2010: Primary 11P70; Secondary 20F05, 20F99, 11B13, 05E15.

It is easy to prove that if S is a finite subset of \mathbb{Z} , then

$$2|S| - 1 \leq |2S| \leq \frac{|S|(|S| + 1)}{2}.$$

Moreover $|2S| = 2|S| - 1$ if and only if S is a (finite) arithmetic progression, that is, a set of the form

$$\{a, a + q, a + 2q, \dots, a + (t - 1)q\}$$

where a , q and t are three integers, $t \geq 1$, $q \geq 0$. The parameter t is called the *size* of the arithmetic progression and q its *difference* (we shall use *ratio* in the multiplicative notation). In the articles [4] and [5], G.A. Freiman proved the following more general results. The first result is referred to as the $3k - 4$ theorem.

Theorem A. *Let S be a finite set of integers with at least three elements. If $|2S| \leq 3|S| - 4$, then S is contained in an arithmetic progression of size $|2S| - |S| + 1 \leq 2|S| - 3$.*

The second result goes one step further. It is called the $3k - 3$ theorem.

Theorem B. *Let S be a finite set of integers with at least 3 elements. If $|2S| = 3|S| - 3$, then one of the following holds:*

- (i) S is a subset of an arithmetic progression of size at most $2|S| - 1$,
- (ii) S is the union of two arithmetic progressions with the same difference,
- (iii) $|S| = 6$ and S is Freiman-isomorphic to the set K_6 , where

$$K_6 = \{(0, 0), (1, 0), (2, 0), (0, 1), (0, 2), (1, 1)\}.$$

Recall that two sets are Freiman isomorphic if they behave with respect to addition in the same way (there is a one-to-one correspondence between the two sets as well as between their two sumsets). Notice that translations and dilations are transformations which send a set on another set which is Freiman isomorphic to it. For instance, in case (iii) of the above-stated theorem, such a set S of integers is, up to translation and dilation, of the form

$$\{0, 1, 2, u, u + 1, 2u\}$$

for an integer $u \geq 5$.

Freiman also investigated in these papers the exact structure of subsets S of the additive group \mathbb{Z} if $|2S| = 3|S| - 2$ (Theorem $3k - 2$) and more generally of small doubling sumsets of \mathbb{Z}^d (see for instance [25]).

Since then, far-reaching generalizations have been obtained, see [3]. Although very powerful and general, these last results are not very precise.

In papers [8], [9], [10], [11] and [12], we started the precise investigation of small doubling problems for subsets of an ordered group. We recall that if G

is a group and \leq is a total order relation defined on the set G , then (G, \leq) is an *ordered group* if for all $a, b, x, y \in G$ the inequality $a \leq b$ implies that $xay \leq xby$, and a group G is *orderable* if there exists an order \leq on the set G such that (G, \leq) is an ordered group. Obviously the group of integers with the usual ordering is an ordered group. More generally, it is possible to prove that a nilpotent group is orderable if and only if it is torsion-free (see, for example, [18] or [20]).

Extending Freiman's results, we proved in [8] (Corollary 1.4) the following theorem, which is analogous to the $3k - 4$ theorem.

Theorem C. *Let G be an orderable group and let S be a finite subset of G with at least three elements. If $|S^2| \leq 3|S| - 4$, then $\langle S \rangle$ is abelian. Moreover, there exists elements x_1 and g in G , such that $gx_1 = x_1g$ and S is a subset of*

$$\{x_1, x_1g, x_1g^2, \dots, x_1g^u\}$$

where $u = |S^2| - |S|$. In other words, S is contained in an abelian geometric progression of size $|S^2| - |S| + 1$.

Furthermore, in the case when $|S^2| = 3|S| - 3$, we obtained the following initial result (this is our Theorem 1.3 in [8])

Theorem D. *Let G be an orderable group and let S be a finite subset of G of size at least 3. If $|S^2| \leq 3|S| - 3$, then $\langle S \rangle$ is abelian.*

Using results of Freiman and Stanchescu, we proved in [12] (Theorem 1) the following theorem concerning the more precise structure of such small doubling sets S .

Theorem E. *Let G be an orderable group and let S be a finite subset of G of size at least 3 satisfying $|S^2| \leq 3|S| - 3$. Then $\langle S \rangle$ is abelian and at most 3-generated.*

Moreover, if $|S| \geq 11$, then one of the following two possibilities occurs:

- (i) S is a subset of a geometric progression of length at most $2|S| - 1$,
- (ii) S is a union of two geometric progressions with the same ratio.

We also proved the following result concerning the structure of $\langle S \rangle$ in the case when $|S^2| = 3|S| - 2$ (see [12], Theorems 2 and 5). To state it, recall the important notation

$$[a, b] = a^{-1}b^{-1}ab \quad \text{and} \quad a^b = b^{-1}ab.$$

Theorem F. *Let G be an orderable group and let S be a finite subset of G of size at least 3.*

If $|S^2| = 3|S| - 2$, then one of the following holds:

- (i) $\langle S \rangle$ is abelian and at most 4-generated,

- (ii) $\langle S \rangle = \langle a, b \rangle$, with $[a, b] \neq 1$ and $[[a, b], a] = [[a, b], b] = 1$. In particular, $\langle S \rangle$ is nilpotent of class 2,
- (iii) $\langle S \rangle = \langle a, b \rangle$, with $a^{b^2} = aa^b$ and $[a, a^b] = 1$,
- (iv) $\langle S \rangle = \langle a, b \rangle$, with $a^b = a^2$. In particular, $\langle S \rangle$ is a quotient of the Baumslag-Solitar group $B(1, 2)$,
- (v) $\langle S \rangle = \langle a \rangle \times \langle c, b \rangle$, with $c^b = c^2$, $|S| = 4$ and $S = \{a, ac, ac^2, y\}$, where y is a suitable element of $\langle c, b \rangle$.

If $\langle S \rangle$ is an abelian group which is at most 4-generated and $|S^2| = 3|S| - 2$, then the structure of S can be deduced from previous results of Freiman and Stanchescu (see [12], Theorem 2). The aim of this paper is to go one step further in the non-abelian case. Namely, we shall present a complete description of the structure of S if S is a finite subset of an orderable group G with $|S^2| = 3|S| - 2$ and $\langle S \rangle$ is non-abelian. The following result will be our main theorem.

Theorem 1. *Let (G, \leq) be an ordered group and let S be a finite subset of G of size at least 4. We assume that $|S^2| = 3|S| - 2$ and that $\langle S \rangle$ is non-abelian. Then one of the following holds:*

- (i) $S = \{a, ac, \dots, ac^i, b, bc, \dots, bc^j\}$, where $[a, c] = [b, c] = 1, c > 1$ and either $ab = bac$ or $ba = abc$,
- (ii) $S = \{x, xc, xc^2, \dots, xc^{k-1}\}$, where $c > 1$ and either $c^x = c^2$ or $(c^2)^x = c$,
- (iii) $|S| = 4$ and the structure of S is of one of the following types:
 - (a) either $S = \{x, xc, xc^x, xc^{x^2}\}$ or $S = \{x^{-1}, x^{-1}c, x^{-1}c^x, x^{-1}c^{x^2}\}$, with $c > 1$ and $c^{x^2} = cc^x = c^xc$,
 - (b) $S = \{1, c, c^2, x\}$, where either $c^x = c^2$ or $(c^2)^x = c$,
 - (c) $S = \{x, xc, xc^2, y\}$, where $[c, x] = 1$ and either $[x, y] = c = (c^2)^y$ or $[y, x] = c^2 = c^y$,
 - (d) $S = \{x, xc, xc^2, y\}$, where $[c, x] = [x, y] = 1$ and either $c^y = c^2$ or $(c^2)^y = c$.

Moreover, if either (i) or (ii) or case (b) of (iii) holds, then $|S^2| = 3|S| - 2$.

This paper is organized as follows. In Section 2, we record some useful results from [12] and [11]. In Section 3, we first study the group $\langle a, b \mid a^{b^2} = aa^b, [a, a^b] = 1 \rangle$. Then we investigate the structure of S if $\langle S \rangle = \langle a, b \mid a^{b^2} = aa^b, [a, a^b] = 1 \rangle$ and $|S^2| = 3|S| - 2$. We prove in Theorem 2 that these assumptions imply that $|S| \leq 4$ and we present a complete description of S if $|S| = 4$ and $|S^2| = 10$. In Section 4 we record some basic results concerning the Baumslag-Solitar group $B(1, 2)$, mainly from [10]. Then we present in Theorem 3 a complete description of subsets S of $B(1, 2)$ satisfying $\langle S \rangle = G$

and $|S^2| = 3|S| - 2$. Notice that small doubling problems in the Baumslag-Solitar groups have been also studied in [9]. Finally, in Section 5 we prove Theorem 1. We refer to books [2], [6] [21] and [22] for notation and definitions.

2. SOME USEFUL RESULTS

Here we collect the following useful results from [12] and [11].

Proposition 1 (see [12], Lemma 4). *Let G be an orderable group and let S be a finite subset of G of size at least 2. If T denotes $S \setminus \{\max S\}$, then either $\langle S \rangle$ is a 2-generated abelian group, or $|T^2| \leq |S^2| - 3$.*

In the next proposition, we use the notation $\dot{\cup}$ for a disjoint union.

Proposition 2 (see [12], Proposition 3). *Let G be an orderable group and let S be a finite subset of G of size at least 3 satisfying $|S^2| = 3|S| - 2$. Suppose that $S = T \dot{\cup} \{y\}$, where $\langle T \rangle$ is abelian. Then either $\langle S \rangle$ is abelian, or*

$$S = \{x, xc, \dots, xc^{k-2}, y\}$$

and one of the following holds:

- (i) $[c, x] = [c, y] = 1$ and either $[x, y] = c$ or $[y, x] = c$,
- (ii) $|S| = 4$, $[c, x] = 1$ and either $[x, y] = c = (c^2)^y$ or $[y, x] = c^2 = c^y$,
- (iii) $|S| = 4$, $[c, x] = [x, y] = 1$ and either $c^y = c^2$ or $(c^2)^y = c$.

The following two propositions deal with the case when $|S| = 3$.

Proposition 3 (see [12], Proposition 1). *Let (G, \leq) be an ordered group and let x_1, x_2, x_3 be three elements of G such that $x_1 < x_2 < x_3$. Let $S = \{x_1, x_2, x_3\}$. Suppose that $\langle S \rangle$ is non-abelian and either $x_1x_2 = x_2x_1$ or $x_2x_3 = x_3x_2$. Then $|S^2| = 7$ if and only if one of the following holds:*

- (i) $S \cap Z(\langle S \rangle) \neq \emptyset$,
- (ii) S is of the form $\{a, a^b, b\}$, where $aa^b = a^ba$.

Proposition 4 (see [12], Proposition 2). *Let (G, \leq) be an ordered group, and let x_1, x_2, x_3 be three elements of G such that $x_1 < x_2 < x_3$. Let $S = \{x_1, x_2, x_3\}$ and assume that $x_1x_2 \neq x_2x_1$ and $x_2x_3 \neq x_3x_2$. If $|S^2| = 7$, then one of the following statements holds:*

- (i) either $S = \{x, xc, xc^x\}$ or $S = \{x^{-1}, x^{-1}c, x^{-1}c^x\}$, with $c > 1$, $c \in G'$ and $c^{x^2} = cc^x = c^xc$,
- (ii) either $S = \{x, xc, xcc^x\}$ or $S = \{x^{-1}, x^{-1}c, x^{-1}cc^x\}$, with $c > 1$, $c \in G'$ and $c^{x^2} = cc^x = c^xc$,
- (iii) $S = \{x, xc, xc^2\}$, with either $c^x = c^2$ or $(c^2)^x = c$.

Next proposition considers the case when $|S| = 4$.

Proposition 5 (see [12], Lemma 6). *Let (G, \leq) be an ordered group and let x_1, x_2, x_3, x_4 be four elements of G such that $x_1 < x_2 < x_3 < x_4$. Let $S = \{x_1, x_2, x_3, x_4\}$ and suppose that $|S^2| = 10$. If $x_2x_3 = x_3x_2$, then either $\langle x_2, x_3, x_4 \rangle$ or $\langle x_1, x_2, x_3 \rangle$ is abelian.*

The final proposition which we shall need deals with the case of nilpotent groups of class 2.

Proposition 6 (see [11], Theorem 3.2). *Let G be an orderable nilpotent group of class 2 and let S be a finite subset of G of size at least 4, such that $\langle S \rangle$ is non-abelian. Then $|S^2| = 3|S| - 2$ if and only if $S = \{a, ac, \dots, ac^i, b, bc, \dots, bc^j\}$, with $c > 1$ and either $ab = bac$ or $ba = abc$.*

3. SUBSETS OF THE GROUP $G = \langle a, b \mid a^{b^2} = aa^b, aa^b = a^ba \rangle$

In this section we shall prove the following theorem.

Theorem 2. *Let*

$$G = \langle a, b \mid a^{b^2} = aa^b, aa^b = a^ba \rangle.$$

- (i) *The group G is orderable.*
Let \leq be a total order on G .
- (ii) *Let S be a finite subset of G satisfying $\langle S \rangle = G$ and $|S^2| = 3|S| - 2$. Then $|S| \leq 4$.*
- (iii) *Moreover, in the case when $|S| = 4$, then either $S = \{x, xc, xc^x, xc^{x^2}\}$ or $S = \{x^{-1}, x^{-1}c, x^{-1}c^x, x^{-1}c^{x^2}\}$, with $c > 1$ and $c^{x^2} = cc^x = c^xc$.*

Throughout this section, we shall denote by G the following group:

$$G = \langle a, b \mid a^{b^2} = aa^b, aa^b = a^ba \rangle.$$

We begin with some remarks concerning G .

Define $H = (\langle u \rangle \times \langle v \rangle) \rtimes \langle t \rangle$, where t, u, v have infinite order and $u^t = v$, $v^t = uv$. Then the defining relations of G hold in H , namely $[u, u^t] = 1$ and $u^{t^2} = uu^t$ and by von Dyck's theorem (Theorem 2.2.1 in [22]) there is an epimorphism $\theta : G \rightarrow H$ with $a^\theta = u$ and $b^\theta = t$. Since $\ker \theta = 1$, it follows that

$$G = (\langle a \rangle \times \langle a^b \rangle) \rtimes \langle b \rangle, \text{ with } a^{b^2} = aa^b.$$

Thus $G' = \langle a \rangle \times \langle a^b \rangle$ and G is a polycyclic metabelian group.

We have $a^{b^2} = aa^b$, $a^{b^3} = a(a^b)^2$ and it is easy to see, by induction on n , that

$$(1) \quad a^{b^n} = a^{f_{n-1}}(a^b)^{f_n} \text{ for any } n \in \mathbb{N},$$

where $(f_n)_{n \in \mathbb{N}_0}$ is the Fibonacci sequence defined in the standard way by induction by $f_0 = 0$, $f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$ for $n > 0$. In particular, $f_2 = 1$ and $a^{b^2} = a^{b+1}$.

Furthermore, recall that a group is called an R^* -group if

$$g^{x_1} \dots g^{x_n} = e \text{ implies } g = e \text{ for all } n \in \mathbb{N} \text{ and all } g, x_1, \dots, x_n \in G.$$

Since metabelian R^* -groups are orderable (see [2], Theorem 4.2.2), in order to prove that G is orderable it suffices to show that it is an R^* -group. This is what we do now.

Proposition 7. *G is an R^* -group and hence it is orderable.*

Proof. It suffices to show that, if $n \in \mathbb{N}$, $k, u, v \in \mathbb{Z}$ and $g_i \in G$, then

$$(b^k a^u (a^b)^v)^{g_1} \dots (b^k a^u (a^b)^v)^{g_r} = 1$$

implies that $b^k a^u (a^b)^v = 1$.

First we notice that by working mod G' it follows that $k = 0$. Hence we may assume that

$$(2) \quad (a^u (a^b)^v)^{b^{n_1}} (a^u (a^b)^v)^{b^{n_2}} \dots (a^u (a^b)^v)^{b^{n_r}} = 1,$$

where $n_i \geq 2$, applying conjugation by a power of b , if necessary. Since by (1)

$$a^{b^{n_1} + b^{n_2} + \dots + b^{n_r}} = a^{c+db}$$

where c, d are positive integers, relation (2) now becomes

$$(a^u)^{c+db} (a^v)^{cb+db^2} = 1.$$

Equivalently

$$a^{uc+udb} a^{vcb+vd(b+1)} = 1,$$

or

$$a^{(uc+vd)+(ud+vc+vd)b} = 1.$$

Hence we have

$$uc + vd = 0 \quad \text{and} \quad ud + vc + vd = 0$$

which implies that

$$ud^2 + (-uc)c + d(-uc) = 0.$$

If $u = 0$, then $vd = 0$ and $v = 0$, so we are done. Hence we may assume that $u \neq 0$. It follows that

$$d^2 - dc - c^2 = 0.$$

Therefore d/c , which is rational, must satisfy

$$\frac{d}{c} = \frac{1 + \sqrt{5}}{2},$$

a contradiction. □

Corollary 1. *Part (i) of Theorem 2 holds.*

Moreover, the following property holds in G .

Proposition 8. *We have $C_{G'}(g) = \{1\}$ for any $g \in G \setminus G'$. In particular $Z(G) = \{1\}$.*

Proof. Let $g \in G \setminus G'$. Then $g = db^n$, where $d \in G'$ and n is an integer different from 0. Since d centralizes G' , it suffices to show that $C_{G'}(b^n) = \{1\}$, where n is a positive integer different from 0.

Denote the element $a^u(a^b)^v$ of G' by (u, v) , where u, v are integers. Then b acts on (u, v) by conjugation via the following function:

$$(u, v)^b = (0 \cdot u + 1 \cdot v, 1 \cdot u + 1 \cdot v) = (u, v)B$$

where

$$B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Thus, by induction, b^n acts by conjugation on (u, v) via multiplication by:

$$B^n = \begin{bmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{bmatrix},$$

where $(f_m)_{m \in \mathbb{N}_0}$ is the Fibonacci sequence.

If b^n centralizes a non-trivial element of G' , then 1 would be an eigenvalue of B^n . But the characteristic polynomial of B^n is $x^2 - (f_{n-1} + f_{n+1})x + (f_{n-1}f_{n+1} - f_n^2)$, which has roots $(f_{n-1} + f_{n+1} \pm \sqrt{5}f_n)/2$, which are irrational for $n > 0$. Hence $C_{G'}(b^n) = \{1\}$, as required. \square

Now, let \leq be a total order in G such that (G, \leq) is an ordered group. Let $S = \{x_1, x_2, \dots, x_k\}$ be a subset of G of size k and suppose that $x_1 < x_2 < \dots < x_k$. We wish to study the structure of S if $|S^2| = 3|S| - 2$. We begin with the case $k = 3$.

Proposition 9. *Let $S \subseteq G$, with $\langle S \rangle = G$. Suppose that $|S| = 3$. Then $|S^2| = 7$ if and only if one of the following holds:*

- (i) $S = \{1, x, y\}$, with $xy \neq yx$,
- (ii) $S = \{c, c^t, t\}$, with $cc^t = c^tc$,
- (iii) either $S = \{t, tc, tc^t\}$ or $S = \{t, tc, tc^{t^2}\}$, where $c \in G'$, $c > 1$ and $c^{t^2} = cc^t = c^tc$,
- (iv) either $S = \{t^{-1}, t^{-1}c, t^{-1}c^t\}$ or $S = \{t^{-1}, t^{-1}c, t^{-1}c^{t^2}\}$, where $c \in G'$, $c > 1$ and $c^{t^2} = cc^t = c^tc$.

Furthermore, in any case, either $S \cap G' \subseteq \{1\}$ or $|S \cap G'| = 2$.

Proof. Suppose that $S = \{x_1, x_2, x_3\}$ and $|S^2| = 7$. If either $x_1x_2 = x_2x_1$ or $x_2x_3 = x_3x_2$ holds, then either (i) or (ii) holds by Proposition 3, since $Z(G) = \{1\}$.

If $x_1x_2 \neq x_2x_1$ and $x_2x_3 \neq x_3x_2$, then either (iii) or (iv) holds by Proposition 4, since the relation $c^x = c^2$ is impossible in a torsion-free polycyclic group (otherwise there would be an infinite chain of subgroups of G : $\langle c \rangle \subset \langle c^{x^{-1}} \rangle \subset \langle c^{x^{-2}} \rangle \subset \dots \subset \langle c^{x^{-n}} \rangle \subset \dots$).

In particular, if (i) holds, then either $S \cap G' = \{1\}$ or $S \cap G' = \{1, z\}$ with $z \in \{x, y\}$, since G' is abelian and G is non-abelian. In case (ii), $c^t = cd$ with $d \in G' \setminus \{1\}$ and $cc^t = c^tc$ implies that $cd = dc$. Hence, by Proposition 8, $c \in S \cap G'$ and since $c^t \neq c$, it follows that $t \notin S \cap G'$. Thus $S \cap G' = \{c, c^t\}$. In cases (iii) and (iv) $c, c^t, c^{t^2} \in G'$, so $t \notin G'$ since G is non-abelian. Hence $S \cap G' = \emptyset$ in these cases. Thus in all cases either $S \cap G' \subseteq \{1\}$ or $|S \cap G'| = 2$ holds.

A direct calculation proves the converse of the main statement. \square

Now we study the structure of S if $|S| = 4$ and $|S^2| = 10$. We begin with the following four lemmas.

Lemma 1. *Let $S = \{t, tc, tc^t, x_4\} \subseteq G$, with $c^{t^2} = c^tc = cc^t$ and $t < tc < tc^t < x_4$. Then $|S^2| = 10$ if and only if $x_4 = tc^{t^2}$.*

Proof. Suppose that $|S^2| = 10$. Write $x_1 = t, x_2 = tc, x_3 = tc^t$ and $T = \{x_1, x_2, x_3\}$. Then

$$T^2 = \{t^2, t^2c, t^2c^t, t^2cc^t, t^2c^tc^t, t^2c^2c^t, t^2c(c^t)^2\}.$$

Notice that $c = (c^t)^{-1}(c^t)^t$, implying that c and c^t belong to G' . Moreover, $t \notin G'$ since $c^t \neq c$, and $c > 1$ since $t < tc$.

Obviously $x_3x_4, x_4^2 \notin T^2$ because of the ordering. Hence one of the elements x_1x_4, x_2x_4 belongs to T^2 , since $|T^2| = 7$ and $|S^2| = 10$. Thus $x_4 = td$ for some $d \in G'$. If $x_3x_4 = x_4x_3$, then $t(d(c^t)^{-1}) = ((c^t)^{-1}d)t = (d(c^t)^{-1})t$ and $d = c^t$ by Proposition 8. But then $x_3 = x_4$, a contradiction. Hence $x_3x_4 \neq x_4x_3$ and

$$S^2 = T^2 \dot{\cup} \{x_3x_4, x_4x_3, x_4^2\}.$$

Notice that

$$\begin{aligned} x_1x_4 &= t^2d, & x_2x_4 &= t^2c^td, & x_3x_4 &= t^2cc^td, \\ x_4x_1 &= t^2d^t, & x_4x_2 &= t^2d^tc & \text{and} & & x_4x_3 &= t^2d^tc^t. \end{aligned}$$

If $x_2x_4 \notin T^2$, then the only possibility is $x_2x_4 = x_4x_3$, thus $t^2c^td = t^2d^tc^t$ and $d^t = d$, a contradiction. Therefore $x_2x_4 \in T^2$ and the only possibilities are $d = c^2$ or $d = cc^t$, since $c^t < d$. If $d = c^2$, then $x_1x_4 = t^2c^2 \notin T^2$ and the only possibility is $x_1x_4 = x_4x_3$, yielding $d = d^tc^t$ and $c^2 = (c^t)^3$, a contradiction since $c < c^t$. Therefore the only remaining possibility is $d = cc^t$ and $x_4 = tc^{t^2}$, as required.

A direct calculation proves the converse. \square

Lemma 2. Let $S = \{t^{-1}, t^{-1}c, t^{-1}c^t, x_4\} \subseteq G$, with $c^{t^2} = c^t c = cc^t$ and $t^{-1} < t^{-1}c < t^{-1}c^t < x_4$. Then $|S^2| = 10$ if and only if $x_4 = t^{-1}c^{t^2}$.

Proof. Suppose that $|S^2| = 10$. As in the previous lemma, we may assume that $x_4 = t^{-1}d$, where $d \in G'$. Notice also that $c, c^t \in G'$ and G' is abelian. Write

$$\bar{S} = \{t, tc, tc^t, td\}.$$

Then

$$\begin{aligned} |\bar{S}^2| &= |t\{1, c, c^t, d\}t\{1, c, c^t, d\}| \\ &= |t^2\{1, c, c^t, d\}^t\{1, c, c^t, d\}| \\ &= |\{1, c, c^t, d\}\{1, c, c^t, d\}^{t^{-1}}| \\ &= |\{1, c, c^t, d\}^{t^{-1}}\{1, c, c^t, d\}| \\ &= |t^{-2}\{1, c, c^t, d\}^{t^{-1}}\{1, c, c^t, d\}| \\ &= |S^2|. \end{aligned}$$

Therefore $|\bar{S}^2| = 10$ and $d = cc^t = c^{t^2}$ by the previous lemma.

A direct calculation proves the converse. \square

Lemma 3. Let $S = \{t, tc, tc^{t^2}, x_4\} \subseteq G$, with $c^{t^2} = c^t c = cc^t$ and $t < tc < tc^{t^2} < x_4$. Then $|S^2| > 10$.

Proof. Write $x_1 = t, x_2 = tc, x_3 = tc^{t^2}$ and $T = \{x_1, x_2, x_3\}$. Then

$$T^2 = \{t^2, t^2c, t^2c^t, t^2cc^t, t^2(c^t)^2c, t^2c^2(c^t)^2, t^2c^2(c^t)^3\}$$

and, as in Lemma 1, $c > 1$, $c, c^t \in G'$ and $t \notin G'$. Thus, by Proposition 8, $\langle S \rangle$ is non-abelian and by Theorem D $|S^2| \geq 3|S| - 2 = 10$. So it suffices to assume that $|S^2| = 10$ and to reach a contradiction.

Obviously $x_3x_4, x_4^2 \notin T^2$ because of the ordering. Hence one of the elements x_1x_4, x_2x_4 belongs to T^2 , since $|T^2| = 7$ and $|S^2| = 10$. It follows, as in Lemma 1, that $x_4 = td$ for some $d \in G'$ and $x_3x_4 \neq x_4x_3$. Thus

$$S^2 = T^2 \cup \{x_3x_4, x_4x_3, x_4^2\}$$

and

$$\begin{aligned} x_1x_4 &= t^2d, & x_2x_4 &= t^2c^td, & x_3x_4 &= t^2(c^t)^2cd, \\ x_4x_1 &= t^2d^t, & x_4x_2 &= t^2d^tc & \text{and} & & x_4x_3 &= t^2d^tc^t. \end{aligned}$$

If $x_2x_4 \notin T^2$, then the only possibility is $x_2x_4 = x_4x_3$. But then $tctd = tdtc^{t^2}$ and $c^td = (c^td)^t$, in contradiction to Proposition 8. Thus $x_2x_4 \in T^2$, which implies that either $d = c^2c^t$ or $d = c^2(c^t)^2$, since $c^t < d$.

In the first case $x_1x_4 = t^2c^2c^t \notin T^2$, thus $x_1x_4 = x_4x_3$ and $d = d^tc^tc$. But $d = c^2c^t$, so $d^t = c$ and $c = d^t = (c^t)^2c^{t^2} = (c^t)^3c$ since $c^{t^2} = c^t c$, a contradiction.

If, on the other hand, $d = c^2(c^t)^2$, then $x_4x_1 = t^2c^2(c^t)^4 \notin T^2$, so $x_4x_1 = x_3x_4$ and $d^t = c(c^t)^2d$. Thus $c^2(c^t)^4 = c^3(c^t)^4$, again a contradiction.

We have reached a contradiction in all possible cases and our Lemma is proved. \square

Lemma 4. *Let $S = \{t^{-1}, t^{-1}c, t^{-1}c^{t^2}, x_4\} \subseteq G$, with $c^{t^2} = c^tc = cc^t$ and $t^{-1} < t^{-1}c < t^{-1}c^t < x_4$. Then $|S^2| > 10$.*

Proof. We can argue as in Lemma 2, using the result of Lemma 3. \square

Now we can prove part (iii) of Theorem 2.

Proof of Theorem 2 (iii). Suppose that $|S^2| = 10$. Write, as usual, $S = \{x_1, x_2, x_3, x_4\}$, $x_1 < x_2 < x_3 < x_4$, $T = \{x_1, x_2, x_3\}$ and $V = \{x_2, x_3, x_4\}$.

If $S = A \dot{\cup} \{y\}$ with $\langle A \rangle$ abelian, then by Proposition 2, either (i) of that proposition holds, in contradiction to Proposition 8, or one of (ii) and (iii) holds, in which case either $c^y = c^2$ or $(c^2)^y = c$, which as shown in the proof of Proposition 9, is impossible in a polycyclic torsion-free group. Therefore we may assume that each triple of elements in S generates a non-abelian group. In particular, $\langle T \rangle$ and $\langle V \rangle$ are non-abelian. By Proposition 1 $|T^2| \leq 7$ and since $\langle T \rangle$ is non-abelian, Theorem D implies that $|T^2| = 7$.

Therefore $|S^2| = |T^2| + 3$ and $\langle T \rangle$ is non-abelian. The elements x_3x_4, x_4^2 are not in T^2 because of the ordering, so one of the elements x_1x_4, x_2x_4 belongs to T^2 . Hence $x_4 \in \langle T \rangle$ and $G = \langle T \rangle$. Arguing similarly, it follows that $|V^2| = 7$, $\langle V \rangle$ is non-abelian and $G = \langle V \rangle$. Therefore T and V satisfy the hypotheses of Proposition 9.

If $1 \in T$, then $1 = x_1$ by Proposition 5, and V satisfies either (ii) or (iii) or (iv) of Proposition 9. If V satisfies (ii), then $|V \cap G'| = 2$ and $|S \cap G'| = 3$, a contradiction, since G' is abelian. If V satisfies either (iii) or (iv) of Proposition 9, then $S^2 = V^2 \dot{\cup} V \dot{\cup} \{1\}$ and $|S^2| = 11$, a contradiction. Therefore we may assume that $1 \notin T$ and T satisfies either (ii) or (iii) or (iv) of Proposition 9.

If T satisfies (ii) of Proposition 9, then $|T \cap G'| = 2$ and hence $|V \cap G'| \geq 1$. Thus it follows by Proposition 9 that $|V \cap G'| = 2$. If $|T \cap G'| = \{x_2, x_3\}$, then $x_2x_3 = x_3x_2$ and Proposition 5 implies that either $\langle T \rangle$ or $\langle V \rangle$ is abelian, a contradiction. Hence $x_1 \in T \cap G'$ and $|S \cap G'| = 3$, yielding again a contradiction. Consequently T satisfies either (iii) or (iv) of Proposition 9 and thus it is equal to one of the following sets: $\{t, tc, tc^t\}$, $\{t^{-1}, t^{-1}c, t^{-1}c^t\}$, $\{t, tc, tc^{t^2}\}$ and $\{t^{-1}, t^{-1}c, t^{-1}c^{t^2}\}$, where $c \in G'$, $c > 1$ and $c^{t^2} = cc^t = c^tc$. It follows by Lemmas 1, 2, 3 and 4 that T must be equal to one of the first two sets and S is as required.

A direct calculation proves the converse. \square

Finally, we study the case $S \subseteq G$, $|S| = 5$ in the next proposition.

Proposition 10. *Let $S \subseteq G$, with $\langle S \rangle = G$ and suppose that $|S| = 5$. Then $|S^2| > 13 = 3|S| - 2$*

Proof. If $|S| = 5$, then by Theorem D, $|S| \geq 13$. So it suffices to assume that $|S| = 13$ and to reach a contradiction.

Write $S = \{x_1, x_2, x_3, x_4, x_5\}$, $x_1 < x_2 < x_3 < x_4 < x_5$, $T = \{x_1, x_2, x_3, x_4\}$ and suppose that $|S^2| = 13$. Arguing as in the previous proposition, we may conclude that $|T^2| = 10$, $|S^2| = |T^2| + 3$ and $\langle T \rangle = G$. Hence T satisfies the hypotheses of part (iii) of Theorem 2.

Suppose first that $T = \{t, tc, tc^t, tc^{t^2}\}$, with $c > 1$ and $c^{t^2} = cc^t = c^t c$. Then $x_1 = t$, $x_2 = tc$, $x_3 = tc^t$, $x_4 = tc^{t^2}$ and as shown in the proof of Lemma 1, $c, c^t \in G'$ and $t \notin G'$. Moreover,

$$T^2 = \{t^2, t^2 c, t^2 c^t, t^2 c c^t, t^2 c^t c^t, t^2 c c^t c^t, t^2 c^2 c^t, t^2 c^2 c^t c^t, t^2 c(c^t)^3, t^2 c^2(c^t)^3\},$$

and in particular

$$(3) \quad \text{if } t^2 c^\alpha (c^t)^\beta \in T^2, \quad \text{then } \alpha \in \{0, 1, 2\}, \beta \in \{0, 1, 2, 3\}.$$

Since $x_4 x_5 \notin T^2$, at least one of the elements $x_1 x_5, x_2 x_5, x_3 x_5$ belongs to T^2 , implying that

$$x_5 = tc^l (c^t)^m$$

for some integers l and m . We have :

$$\begin{aligned} x_3 x_5 &= t^2 c^{l+1} (c^t)^{1+m}, & x_5 x_3 &= t^2 c^m (c^t)^{l+m+1}, & x_2 x_5 &= t^2 c^l (c^t)^{1+m}, \\ x_5 x_2 &= t^2 c^{m+1} (c^t)^{l+m}, & x_1 x_5 &= t^2 c^l (c^t)^m & \text{and} & \quad x_5 x_1 = t^2 c^m (c^t)^{l+m}. \end{aligned}$$

If each of $x_3 x_5, x_5 x_3, x_2 x_5, x_5 x_2, x_1 x_5, x_5 x_1$ belongs to T^2 , then $l, m \in \{0, 1\}$, since these elements involve $\{c^l, c^m, c^{l+1}, c^{m+1}\}$ and each element of T^2 involves only one of $\{c^0, c, c^2\}$. Hence either $x_5 = t$, or $x_5 = tc$, or $x_5 = tc^t$, or $x_5 = tcc^t = tc^{t^2}$, a contradiction. Therefore there exists $i \in \{1, 2, 3\}$ such that either $x_i x_5 \notin T^2$ or $x_5 x_i \notin T^2$.

Now $x_5 x_4 = t^2 c^{m+1} (c^t)^{l+m+1}$ and $x_4 x_5 = t^2 c^{l+1} (c^t)^{m+2}$. Thus $x_5 x_4 = x_5 x_4$ is impossible, since it implies that $l = m = 1$ and $x_5 = tcc^t = tc^{t^2}$, a contradiction. Hence

$$S^2 = T^2 \dot{\cup} \{x_4 x_5, x_5 x_4, x_5^2\}.$$

If $x_i x_5 \notin T^2$, then the only possibility is $x_i x_5 = x_5 x_4$ and if $x_5 x_i \notin T^2$, then the only possibility is $x_5 x_i = x_4 x_5$.

If $x_3 x_5 = x_5 x_4$, then $l = m = 0$, a contradiction. If $x_2 x_5 = x_5 x_4$, then $l = 0, m = -1$, so $x_5 = t(c^t)^{-1} < t = x_1$, also impossible. If $x_1 x_5 = x_5 x_4$, then $l = -1, m = -2$, so $x_5 = tc^{-1}(c^t)^{-2} < t = x_1$, a contradiction. If $x_5 x_1 = x_4 x_5$, then $l = 2, m = 3$, so $x_5 = tc^2(c^t)^3$ and $x_2 x_5 = t^2 c^2(c^t)^4 \notin T^2$, leading us to a previous case. If $x_5 x_2 = x_4 x_5$, then $l = 2, m = 2$, so $x_5 = tc^2(c^t)^2$

and $x_3x_5 = t^2c^3(c^t)^3 \notin T^2$, leading us again to a previous case. Finally, if $x_5x_3 = x_4x_5$, then $l = 1, m = 2$, so $x_5 = tc(c^t)^2$ and $x_5x_2 = t^2c^3(c^t)^3 \notin T^2$, and again we are in a previous case.

We have reached a contradiction in all cases. Hence if $T = \{t, tc, tc^t, tc^{t^2}\}$, with $c > 1$ and $c^{t^2} = cc^t = c^tc$, then $|S^2| > 13$.

Now suppose that $T = \{t^{-1}, t^{-1}c, t^{-1}c^t, t^{-1}c^{t^2}\}$ with $c > 1$ and $c^{t^2} = cc^t = c^tc$.

Arguing as before we may write $x_5 = t^{-1}c^l(c^t)^m$, for some integers l, m . Write

$$\bar{S} = \{t, tc, tc^t, tc^{t^2}, tc^l(c^t)^m\}.$$

Then

$$\begin{aligned} |\bar{S}^2| &= |t\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}t\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}| \\ &= |t^2\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}^t\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}| \\ &= |\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}^{t^{-1}}| \\ &= |\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}^{t^{-1}}\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}| \\ &= |t^{-2}\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}^{t^{-1}}\{1, c, c^t, c^{t^2}, c^l(c^t)^m\}| \\ &= |S^2|. \end{aligned}$$

But $|\bar{S}^2| > 13$ by the previous paragraph, so $|S^2| > 13$, as required. \square

Now we can conclude the proof of Theorem 2.

Proof of Theorem 2, part (ii). Suppose that $|S| = k \geq 5$ and write

$$S = \{x_1, x_2, \dots, x_{k-1}, x_k\} \quad \text{and} \quad T = \{x_1, x_2, \dots, x_{k-1}\}.$$

Then, by Proposition 1, $|T^2| \leq |S^2| - 3 = 3|T| - 2$. If $|T^2| \leq 3|T| - 3$, then, by Theorem D, $\langle T \rangle$ is abelian and Proposition 2 yields a contradiction, since case (i) of Proposition 2 is impossible as $Z(G) = \{1\}$ by Proposition 8 and as shown in the proof of Proposition 9, cases (ii) and (iii) of Proposition 2 are impossible in a polycyclic torsion-free group.

Thus $|T^2| = 3|T| - 2 = |S^2| - 3$ and since $k - 1 \geq 4$, at least one of the $k - 1$ elements $x_1x_k, x_2x_k, \dots, x_{k-1}x_k$ belongs to T^2 . Hence $x_k \in \langle T \rangle$ and $\langle T \rangle = \langle S \rangle = G$. Thus, by induction, we may assume that $|S| = 5$, in which case we get the contradiction $|S^2| > 13$ by Proposition 10. Therefore $|S| \leq 4$ and the structure of S if $|S| = 4$ follows from part (iii) of Theorem 2. \square

4. SUBSETS OF THE BAUMSLAG-SOLITAR GROUP $BS(1, 2)$

Our aim in this section is to prove the following theorem.

Theorem 3. *Let $G = \langle a, b \mid a^b = a^2 \rangle$ and let S be a generating subset of G . Then the following statements hold:*

- (i) If $|S| > 4$, then $|S^2| = 3|S| - 2$ if and only if $S = \{x, xc, \dots, xc^{k-1}\}$, where $c > 1$ and either $c^x = c^2$ or $(c^2)^x = c$.
- (ii) If $|S| = 4$, then $|S^2| = 3|S| - 2$ if and only if either $S = \{1, c, c^2, x\}$, where either $c^x = c^2$ or $(c^2)^x = c$, or $S = \{x, xc, xc^2, xc^3\}$, where $c > 1$ and either $c^x = c^2$ or $(c^2)^x = c$.

Throughout this section we shall denote by G the Baumslag-Solitar group

$$G = BS(1, 2) = \langle a, b \mid a^b = a^2 \rangle.$$

We begin with some basic well-known results concerning G .

Proposition 11. *The following statements hold:*

- (i) $G' = \langle a^{b^n} \mid n \in \mathbb{Z} \rangle$ is abelian,
- (ii) $G = G' \rtimes \langle b \rangle$,
- (iii) G is orderable,
- (iv) If $c \in G'$, then $c^b = c^2$,
- (v) $C_{G'}(g) = \{1\}$ for any $g \in G \setminus G'$. In particular $Z(G) = \{1\}$.

Proof. Clearly $G' = a^G = \langle a^{b^n} \mid n \in \mathbb{Z} \rangle$. For claims (i)-(iv), see Theorem 10 in [10] and its proof.

Concerning (v), let $g \in G \setminus G'$, $c \in G'$ and suppose that $c^g = c$. By (i) $g = db^s$ for some $s \in \mathbb{Z} \setminus \{0\}$ and $c^g = c$ implies that $c^{b^s} = c$. We may assume that $s \geq 1$ and by (iv) we obtain $c^{2^s} = c$. Since $2^s > 1$, it follows that $c = 1$, as required. \square

Now, let \leq be a total order in G such that (G, \leq) is an ordered group. Let $S = \{x_1, x_2, \dots, x_k\}$ be a subset of G of order k and suppose that $x_1 < x_2 < \dots < x_k$. We study the structure of S if $|S^2| = 3|S| - 2$. We begin with the case $k = 3$.

Proposition 12. *Let $S \subseteq G$, with $\langle S \rangle = G$ and $|S| = 3$. Then $|S^2| = 7$ if and only if one of the following holds:*

- (i) $S = \{1, x, y\}$, with $xy \neq yx$,
- (ii) $S = \{c, c^t, t\}$, with $cc^t = c^t c$ and $c, c^t \in G'$,
- (iii) $S = \{x, xc, xc^2\}$, where $c > 1$ and either $c^x = c^2$ or $(c^2)^x = c$.

Furthermore, in any case, either $S \cap G' \subseteq \{1\}$ or $|S \cap G'| = 2$.

Proof. Suppose that $S = \{x_1, x_2, x_3\}$ and $|S^2| = 7$. If either $x_1 x_2 = x_2 x_1$ or $x_2 x_3 = x_3 x_2$, then either (i) or (ii) holds by Proposition 3, since $Z(G) = \{1\}$.

If $x_1 x_2 \neq x_2 x_1$ and $x_2 x_3 \neq x_3 x_2$, then (iii) holds by Proposition 4. In fact, cases (i) and (ii) of Proposition 4 cannot occur, since the relation $c^{x^2} = cc^x$ with $c > 1$ is impossible in the group $BS(1, 2)$. For, if $c^{x^2} = cc^x$, then c^x and hence c belong to G' and by Proposition 11 (iv) $c^b = c^2$. Clearly $x \notin G'$, so

we may assume that $x = b^s$ for some $s \in \mathbb{Z} \setminus \{0\}$. If $x = b^s$ with $s \geq 1$, then $c^x = c^{b^s} = c^{2^s}$, $c^{x^2} = c^{4^s}$ and since $c^{x^2} = c^x c$, we get $c^{4^s} = c^{2^s+1}$. But $c > 1$, so $4^s = 2^s + 1$, a contradiction. Similarly, if $x = b^{-s}$ with $s > 0$, then $c^{x^2} = c c^x$ implies $c = c^{x^{-2}} c^{x^{-1}} = c^{4^s} c^{2^s}$ and since $c > 1$, we get the contradiction $1 = 4^s + 2^s$. So it follows that one of (i), (ii) or (iii) must hold.

In particular, if (i) holds, then either $S \cap G' = \{1\}$ or $S \cap G' = \{1, z\}$ with $z \in \{x, y\}$, since G' is abelian, and $|S \cap G'| = 2$, as required.

In case (ii), $c^t = c c^t c^{-1} = c d$ with $d \in G' \setminus \{1\}$ and $c c^t = c^t c$ implies that $c d = d c$. Hence, by Proposition 11 (v), $c \in S \cap G'$ and since $c^t \neq c$, it follows that $t \notin S \cap G'$. Thus $S \cap G' = \{c, c^t\}$ and $|S \cap G'| = 2$, as required.

Finally, if case (iii) holds, then $c \in G'$ and $x \notin G'$ since $[c, x] \neq 1$. Hence $S \cap G' = \emptyset$, as required.

A direct calculation proves the converse of the main statement. \square

Now we study the structure of S if $k \geq 4$. We begin with the case $S = A \dot{\cup} \{y\}$, where $\langle A \rangle$ is abelian.

Proposition 13. *Let $S \subseteq G$, with $\langle S \rangle = G$. Suppose that $|S| = k \geq 4$ and $S = A \dot{\cup} \{y\}$ with $\langle A \rangle$ abelian. Then $|S^2| = 3|S| - 2$ if and only if $k = 4$ and $S = \{1, c, c^2, y\}$, with either $c^y = c^2$ or $(c^2)^y = c$.*

Proof. Suppose that $|S^2| = 3|S| - 2$. Since $Z(G) = \{1\}$, $\langle S \rangle = G$ is not a nilpotent group of class at most 2 and by Proposition 2 we have $|S| = 4$, $S = \{x, xc, xc^2, y\}$ and either (ii) or (iii) of Proposition 2 holds. If (iii) holds, then $x \in Z(G) = \{1\}$ and $x = 1$. Thus S has the required structure in this case.

Now suppose that (ii) of Proposition 2 holds. Then $c \in G'$ and by Proposition 11 (v) $x \in C_G(c) \subseteq G'$. Moreover, $y \notin G'$ since G' is abelian. Hence, by Proposition 11 (ii), $y = e b^s$ for some $s \in \mathbb{Z} \setminus \{0\}$ and $e \in G'$.

If $c^y = c^2$, then $c^{b^s} = c^2$ and since $c^b = c^2$ by Proposition 11 (iv), we must have $s = 1$. Thus $x^y = x^b = x^2$ by Proposition 11 (iv) and $c^2 = [y, x] = (x^{-1})^y x = x^{-2} x = x^{-1}$. Write $d = c^{-1}$. Then $\{x, xc, xc^2, y\} = \{d^2, d, 1, y\}$ with $d^y = d^2$, as required.

If $(c^2)^y = c$, then it follows that $(c^2)^{b^s} = c$ and the only possibility for s is $s = -1$. Now $x^b = x^2$, so $(x^2)^y = (x^2)^{b^{-1}} = x$ and $(c^2)^y = c = [x, y] = x^{-1} x^y$. Thus $x^y = xc$ and $x = (x^2)^y = xcxc = x^2 c^2$, yielding $x = c^{-2}$. Write $d = c^{-1}$. Then $\{x, xc, xc^2, y\} = \{d^2, d, 1, y\}$ with $(d^2)^y = (d^2)^{b^{-1}} = d$, as required.

A direct calculation proves the converse. \square

We can now describe the structure of S if $k = 4$.

Proposition 14. *Let $S \subseteq G$, with $\langle S \rangle = G$ and suppose that $|S| = 4$. Then $|S^2| = 10$ if and only if one of the following holds:*

- (i) $S = \{1, c, c^2, y\}$, with either $c^y = c^2$ or $(c^2)^y = c$,
- (ii) $S = \{x, xc, xc^2, xc^3\}$, with $c > 1$ and either $c^x = c^2$ or $(c^2)^x = c$.

Proof. Suppose that $S = \{x_1, x_2, x_3, x_4\}$ with $x_1 < x_2 < x_3 < x_4$ and $|S^2| = 10$. Let $T = \{x_1, x_2, x_3\}$ and $V = \{x_2, x_3, x_4\}$. If $S = A \dot{\cup} \{y\}$ with $\langle A \rangle$ abelian, then (i) holds by Proposition 13. Therefore we may assume that each triple of elements in S generates a non-abelian group. In particular, $\langle T \rangle$ and $\langle V \rangle$ are non-abelian.

By Proposition 1 $|T^2| \leq 7$ and since $\langle T \rangle$ is non-abelian, Theorem D implies that $|T^2| = 7$. The elements x_3x_4, x_4^2 are not in T^2 because of the ordering, so one of the elements x_1x_4, x_2x_4 belongs to T^2 , since $|S^2| = |T^2| + 3$. Hence $x_4 \in \langle T \rangle$ and $G = \langle T \rangle$. Arguing similarly, it follows that $|V^2| = 7$ and $\langle V \rangle = G$. Therefore T and V satisfy the hypotheses of Proposition 12.

If $1 \in T$, then $1 = x_1$ by Proposition 5 and V satisfies either (ii) or (iii) of Proposition 12. But then $S^2 = V^2 \dot{\cup} V \dot{\cup} \{1\}$ and $|S^2| = 11$, a contradiction. Therefore we may assume that $1 \notin T$.

Thus, by Proposition 12, T satisfies either (ii) or (iii) of that proposition. If $|T \cap G'| = 2$, then also $|V \cap G'| = 2$ and $V \cap G' \neq \{x_2, x_3\}$ by Proposition 5. Hence $|S \cap G'| = 3$, which is impossible, since $\langle S \cap G' \rangle$ is abelian. Therefore $T \cap G'$ is an empty set and $T = \{x, xc, xc^2\}$, with $c > 1$ and either $c^x = c^2$ or $(c^2)^x = c$.

Suppose, first, that $c^x = c^2$. Then $T^2 = \{x^2, x^2c, x^2c^2, x^2c^3, x^2c^4, x^2c^5, x^2c^6\}$. Obviously $x_4^2 \notin T^2$, because of the ordering. Since $|S^2| = |T^2| + 3$, it follows that one of the elements $xx_4, xc x_4, xc^2 x_4$ belongs to T^2 . Therefore $x_4 = xc^s$ for some integer s . Similarly one of the elements $xc^s x = x^2c^{2s}, xc^s xc = x^2c^{2s+1}, xc^s xc^2 = x^2c^{2s+2}$ belongs to T^2 . Since $x_4 = xc^s > xc^2$ and $c > 1$, we must have $s \geq 3$ and since $x^2c^{2s} \leq x^2c^6$, the only possible case is that $s = 3$. Thus (ii) holds.

Now suppose that $(c^2)^x = c$. In this case

$$T^2 = \{x^2, x^2c, x^2c^2, x^2c^x, x^2c^xc, x^2c^xc^2, x^2c^3\}$$

and, as before, one of the elements x_4x, x_4xc, x_4xc^2 belongs to T^2 . Thus $x_4xc^l = xc^i xc^j$ for some integers i, j, l and $x_4 = xc^i xc^{j-l} x^{-1} = xc^{i+2(j-l)} = xc^s$ for some integer $s \geq 3$, since $x_4 > xc^2$.

Similarly one of the elements $xx_4, xc x_4, xc^2 x_4$ belongs to T^2 . If $xc^2 xc^s \in T^2$, then $x^2c^{s+1} \in T^2$ and $s \leq 2$, a contradiction, and if $xcxc^s \in T^2$, then $x^2c^x c^s \in T^2$ again implying that $s \leq 2$, a contradiction. Therefore the only possible case is that $x^2c^s \in T^2$, forcing $s = 3$ and yielding (ii) again. Thus either (i) or (ii) holds in all cases.

A direct calculation proves the converse. □

Now we can prove Theorem 3.

Proof of Theorem 3. Suppose that $|S| = k \geq 4$ and $|S^2| = 3k - 2$. If $k = 4$, then S has the required structure by Proposition 14. So suppose that $k > 4$.

Write $S = \{x_1, x_2, \dots, x_k\}$, with $x_1 < x_2 < \dots < x_k$, $T = \{x_1, \dots, x_{k-1}\}$ and $V = \{x_2, \dots, x_k\}$. Since $k \geq 5$, it follows by Proposition 13 that each subset of S with $k - 1$ elements generates a non-abelian group. In particular, $\langle T \rangle$ is non-abelian and by Theorem D $|T^2| \geq 3|T| - 2$. But by Proposition 1 $|T^2| \leq |S^2| - 3 = 3|T| - 2$, so it follows that $|T^2| = 3|T| - 2 = |S^2| - 3$. Since $k - 1 \geq 4$, one of the $k - 1$ elements $x_1x_k, x_2x_k, \dots, x_{k-1}x_k$ must belong to T^2 . Hence $x_k \in \langle T \rangle$ and $G = \langle T \rangle$. Similar arguments yield $|V^2| = 3|V| - 2$ and $\langle V \rangle = G$. It follows by induction that either $T = \{x, xc, \dots, xc^{k-2}\}$ with $c > 1$ and either $c^x = c^2$ or $(c^2)^x = c$, or $|T| = 4$ and $T = \{1, c, c^2, y\}$ with either $c^y = c^2$ or $(c^2)^y = c$.

First suppose that the latter case holds. Then $c \in G'$, $|T \cap G'| = 3$ and $|V \cap G'| \geq 2$. But induction applied to V implies that $|V \cap G'| \in \{0, 3\}$, so $|V \cap G'| = 3$. If $T \cap G' \neq V \cap G'$, then $|S \cap G'| = 4 = k - 1$ and we have reached a contradiction, since G' is abelian. Hence $T \cap G' = V \cap G' = \{x_2, x_3, x_4\}$. Now, if one of the elements x_1x_2, x_1x_3, x_1x_4 belongs to $\{x_2, x_3, x_4\}^2$, then $\langle T \rangle$ is abelian and if one of the elements x_2x_5, x_3x_5, x_4x_5 belongs to $\{x_2, x_3, x_4\}^2$, then $\langle V \rangle$ is abelian, a contradiction in both cases. So neither of the above six elements belongs to $\{x_2, x_3, x_4\}^2$ and since $x_1x_2 < x_1x_3 < x_1x_4 < x_2x_5 < x_3x_5 < x_4x_5$, it follows that $|S^2| \geq 6 + |\{x_2, x_3, x_4\}^2| \geq 6 + 5 = 11$, a contradiction.

So we may assume that $T = \{x, xc, \dots, xc^{k-2}\}$, with $c > 1$ and either $c^x = c^2$ or $(c^2)^x = c$. Thus $x_i = xc^{i-1}$ for $i = 1, 2, \dots, k - 1$.

First assume that $c^x = c^2$. Since $|T^2| = |S^2| - 3$ and $k - 1 \geq 4$, there exists an integer i , $1 \leq i \leq k - 1$, such that $xc^ix_k \in T^2$. Hence $xc^ix_k = xc^jxc^l$ for some integers i, j, l and $x_k = c^{j-i}xc^l = xc^{2(j-i)+l} = xc^s$ for an integer s . Now either $x_kx_{k-2} \in T^2$ or $x_kx_{k-2} \notin T^2$.

If $x_kx_{k-2} \in T^2$, then $xc^sxc^{k-3} = xc^rxc^{k-2}$ for some integer r and $x^2c^{2s+k-3} = x^2c^{2r+k-2}$. Thus $2s+k-3 = 2r+k-2$, which is impossible, since these numbers are of different parity.

So suppose that $x_kx_{k-2} \notin T^2$. Then $S^2 \setminus T^2 = \{x_kx_{k-2}, x_kx_{k-1}, x_k^2\}$ and since $x_{k-1}x_k \in S^2 \setminus T^2$, it follows that either $x_{k-1}x_k = x_kx_{k-1}$ or $x_{k-1}x_k = x_kx_{k-2}$. If $x_{k-1}x_k = x_kx_{k-1}$, then $x^2c^{2(k-2)+s} = x^2c^{2s+k-2}$ and $2(k-2)+s = 2s+k-2$, yielding $s = k - 2$ and $x_k \in T$, a contradiction. Hence $x_kx_{k-2} = x_{k-1}x_k$, yielding $2s+k-3 = 2(k-2)+s$. Thus $s = k - 1$, as required.

Now, suppose that $(c^2)^x = c$. Then $c^{x^{-1}} = c^2$ and arguing as in the previous case, there exists i such that $1 \leq i \leq k - 1$ and $x_kxc^i \in T^2$. Hence $x_kxc^i = xc^jxc^l$ for some integers i, j, l and $x_k = xc^jxc^{l-i}x^{-1} = xc^j(c^{l-i})^{x^{-1}} = xc^s$ for some integer s . Now either $xc^{k-3}xc^s \in T^2$ or $xc^{k-3}xc^s \notin T^2$.

If $xc^{k-3}xc^s \in T^2$, then $xc^{k-3}xc^s = xc^{k-2}xc^r$ for some integer r and $xc^s = cxc^r$. Thus $c^{2s}x = c^{1+2r}x$, which is impossible.

Thus $xc^{k-3}xc^s \notin T^2$. Then $S^2 \setminus T^2 = \{x_{k-2}x_k, x_{k-1}x_k, x_k^2\}$ and since $x_kx_{k-1} \in S^2 \setminus T^2$, it follows that either $x_kx_{k-1} = x_{k-1}x_k$ or $x_kx_{k-1} = x_{k-2}x_k$. If $x_kx_{k-1} = x_{k-1}x_k$, then $c^sxc^{k-2} = c^{k-2}xc^s$ and $s + 2(k-2) = k-2 + 2s$. Thus $s = k-2$ and $x_k \in T$, a contradiction. Hence $x_kx_{k-1} = x_{k-2}x_k$, yielding $s + 2(k-2) = k-3 + 2s$. Thus $s = k-1$, as required. The proof in one direction is complete.

Conversely, suppose that $|S| = k$. If $k = 4$ and S satisfies the corresponding conditions, then $|S^2| = 10$ by Proposition 14. If $k > 4$ and $S = \{x, xc, \dots, xc^{k-1}\}$ with $c^x = c^2$, then

$$S^2 = \{xc^i xc^j = x^2 c^{2i+j} \mid 0 \leq i, j \leq k-1\}.$$

We claim that $|S^2| = 3k - 2$. Since $0 \leq 2i + j \leq 3k - 3$, it suffices to show that each integer n with $0 \leq n \leq 3k - 3$ can be represented in the form $n = 2i + j$ for some $0 \leq i, j \leq k-1$. If $n = 0$, then $n = 2 \cdot 0 + 0$ and if $n > 0$, then $n = 3a + b$, where $0 \leq a \leq k-2$ and $1 \leq b \leq 3$. In the latter case, the required representations are: $n = 2a + (a+1)$ if $b = 1$, $n = 2(a+1) + a$ if $b = 2$ and $n = 2(a+1) + (a+1)$ if $b = 3$.

Hence $|S^2| = 3|S| - 2$, as required. If $S = \{x, xc, \dots, xc^{k-1}\}$ with $(c^2)^x = c$, then $c^{x^{-1}} = c^2$ and $x^{-1}S^2x = \{c^i xc^j x = c^{i+2j}x^2 \mid 0 \leq i, j \leq k-1\}$. As shown above $|S^2| = |x^{-1}S^2x| = 3|S| - 2$, as required. \square

5. PROOF OF THEOREM 1

Now we can prove Theorem 1.

Proof of Theorem 1. Let $S \subseteq G$, $|S| = k \geq 4$ and suppose that $|S^2| = 3k - 2$ and $\langle S \rangle$ is non-abelian. Then $\langle S \rangle$ satisfies either (ii), or (iii), or (iv), or (v) of Theorem F. From now on, (ii), (iii), (iv) and (v) denote items of Theorem F and (1i), (1ii) and (1iii) denote items of Theorem 1.

If G is a nilpotent ordered group of class 2 and S is a finite subset of G such that $|S| = k \geq 4$ and $\langle S \rangle$ is non-abelian, then by Proposition 6 $|S^2| = 3k - 2$ if and only if S satisfies (1i). This takes care of $\langle S \rangle$ satisfying (ii), since in cases (iii), (iv) and (v), $\langle S \rangle$ is non-nilpotent. If $\langle S \rangle$ satisfies (iii), then Theorem 2 implies that $k = 4$ and case (a) of (1iii) holds.

Suppose, now, that $\langle S \rangle$ satisfies (iv). Then S satisfies the assumptions of Theorem 3. Hence, if $k > 4$, then $|S^2| = 3k - 2$ if and only if S satisfies (1ii) and if $k = 4$, then $|S^2| = 3k - 2$ if and only if S satisfies either (1ii) or case (b) of (1iii). Notice that if $k = 4$, then the second case in item (ii) of Theorem 3 is of type (1ii).

Finally, if $\langle S \rangle$ satisfies (v), then $|S| = 4$ and $\langle S \rangle$ is not a nilpotent group of class at most 2. Hence, by Proposition 2, S satisfies one of the cases (c) or (d) of (1iii).

Conversely, it follows from our proof that if S satisfies one of the conditions (1i), (1ii) or case (b) of (1iii), then $|S^2| = 3k - 2$. \square

ACKNOWLEDGEMENTS

This work was supported by the "National Group for Algebraic and Geometric Structures, and their Applications" (GNSAGA - INDAM), Italy.

A.P. is supported by the ANR grant Caesar number 12 - BS01 - 0011. He thanks his colleagues from the University of Salerno for their hospitality during the preparation of this paper.

REFERENCES

- [1] Y. Bilu, Structure of sets with small sumset, *Astérisque* **258** (1999), 77–108.
- [2] R. Botto Mura, A. Rhemtulla, Orderable groups, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, 1977.
- [3] E. Breuillard, B. Green, T. Tao, Small doubling in groups, Erdős Centennial, Bolyai Soc. Math. Studies **25**, 2013.
- [4] G.A. Freiman, On the addition of finite sets I, *Izv. Vyss. Ucebn. Zaved. Matematika* **6** (13) (1959), 202–213.
- [5] G.A. Freiman, Inverse problems of additive number theory. IV: On the addition of finite sets. II (Russian), *Elabuž. Gos. Ped. Inst. Učen. Zap.* **8** (1960), 72–116.
- [6] G.A. Freiman, Foundations of a structural theory of set addition, Translations of mathematical monographs **37**, Amer. Math. Soc., Providence, 1973.
- [7] G.A. Freiman, Structure Theory of Set Addition, *Astérisque* **258** (1999), 1–33.
- [8] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, Small doubling in ordered groups, *J. Aust. Math. Soc.* **96** (2014), 316–325.
- [9] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y.V. Stanchescu, Direct and inverse problems in additive number theory and in non-abelian group theory, *Europ. J. Combin.* **40** (2014), 42–54.
- [10] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y.V. Stanchescu, A small doubling structure theorem in a Baumslag-Solitar group, *Europ. J. Combin.* **48** (2015), 106–124.
- [11] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y.V. Stanchescu, Small doubling in ordered nilpotent groups of class 2, submitted.
- [12] G. Freiman, M. Herzog, P. Longobardi, M. Maj, A. Plagne, Y.V. Stanchescu, Small doubling in ordered groups: generators and structure, submitted, (2015) *arXiv:1501.01838*, 25 pages.
- [13] B. Green, What is ... an approximate group?, *Notices Amer. Math. Soc.* **59** (2012), no. 5, 655–656.
- [14] B. Green, I. Z. Ruzsa, Freiman’s theorem in an arbitrary abelian group, *J. London Math. Soc.* **75** (2007), 163–175.
- [15] Y.O. Hamidoune, An application of connectivity theory in graphs to factorizations of elements in groups, *Europ. J. Combin.* **2** (1981), 349–355.

- [16] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 459–484.
- [17] V.F. Lev, P.Y. Smeliansky, On addition of two distinct sets of integers, *Acta Arith.* **70** (1995), no. 1, 85–91.
- [18] A.I. Mal’cev, On ordered groups, *Izv. Akad. Nauk. SSSR Ser. Mat.* **13** (1948), 473–482.
- [19] M.B. Nathanson, Additive Number Theory Inverse Problems and the Geometry of Sumsets, Springer, 1996.
- [20] B.H. Neumann, On ordered groups, *Amer. J. Math.* **71** (1949), 1–18.
- [21] D.J.S. Robinson, Finiteness conditions and generalized soluble groups, Springer-Verlag, Berlin, 1972.
- [22] D.J.S. Robinson, A Course in the Theory of Groups, Springer-Verlag, Berlin, 1995.
- [23] I.Z. Ruzsa, An analog of Freiman’s theorem in groups, *Astérisque* **258** (1999), 323–326.
- [24] T. Sanders, The structure theory of set addition revisited, *Bull. Amer. Math. Soc.* **50** (2013), no. 1, 93–127.
- [25] Y.V. Stanchescu, The structure of d -dimensional sets with small sumset, *J. Number Theory* **130** (2010), no. 2, 289–303.
- [26] T. Tao, V.H. Vu, Additive combinatorics, Cambridge studies in advanced mathematics **105**, 2006.

GREGORY A. FREIMAN, MARCEL HERZOG
 SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, TEL AVIV 69978,
 ISRAEL

E-mail address: grisha@post.tau.ac.il
E-mail address: herzogm@post.tau.ac.il

PATRIZIA LONGOBARDI, MERCEDE MAJ
 DIPARTIMENTO DI MATEMATICA, UNIVERSITA’ DI SALERNO, VIA GIOVANNI PAOLO II,
 132, 84084 FISCIANO (SALERNO), ITALY
E-mail address: plongobardi@unisa.it
E-mail address: mmaj@unisa.it

ALAIN PLAGNE
 CENTRE DE MATHÉMATIQUES LAURENT SCHWARTZ, ÉCOLE POLYTECHNIQUE, 91128
 PALAISEAU CEDEX, FRANCE
E-mail address: plagne@math.polytechnique.fr

DEREK J. S. ROBINSON
 DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN,
 URBANA, IL 61801, USA
E-mail address: dsrobins@illinois.edu

YONUTZ V. STANCHESCU
 AFEKA ACADEMIC COLLEGE, TEL AVIV 69107, ISRAEL
 AND
 THE OPEN UNIVERSITY OF ISRAEL, RAANANA 43107, ISRAEL
E-mail address: yonis@afeka.ac.il and ionut@openu.ac.il